1. Introduction :

La sécurité des ordinateurs, connectés à l'Internet ou non, peut être compromise par un certain nombre de facteurs. Dans cette leçon, nous allons passer en revue les principaux différents dangers qui guettent les utilisateurs, leurs données ou leur porte-feuille. Nous étudierons également les moyens de se prémunir de ces dangers.

2. Qu'est ce qu'un virus informatique ?

Un programme informatique dangereuse avec la caractéristique d'être en mesure de générer des copies de lui-même, et ainsi répandre dans le système informatique. En outre, la plupart des virus informatiques ont une charge destructive qui est activé sous certaines conditions.

Action d'un virus informatique :

Un virus informatique agit selon une méthode tout à fait semblable au virus biologique. C'est d'ailleurs pour cette raison que ce type de programme a été appelé " virus ".

- Le virus informatique injecte le code dont il est formé dans le code d'un programme qu'il trouve sur l'ordinateur cible.
- Lorsque le programme infecté est exécuté, le virus se reproduit et infecte, à nouveau, un ou plusieurs autres programmes.

La particularité des virus informatiques est qu'ils ne peuvent se reproduire sans l'aide d'un programme cible existant.

3. Que font les virus informatiques ?

La présence d'un virus informatique dans un ordinateur peut passer tout à fait inaperçu ou avoir des effets désastreux bien visibles.

Effets des virus

En plus de s'auto-reproduire, un virus aura généralement une autre activité. Celle-ce sera plus ou moins gênante pour l'utilisateur.

Les virus sont capables de :

• S'auto-envoyer sous la forme de courrier électronique aux personnes dont les adresses figurent dans l'ordinateur infecté.
• S'auto-envoyer sous la forme de courrier électronique à des adresses fabriquées
• Utiliser l'ordinateur infecté pour lancer une attaque contre un ordinateur connecté à l'Internet
• Modifier ou supprimer des données dans l'ordinateur infecté.
• Provoquer une panne matérielle.
• Ralentir ou bloquer l'ordinateur infecté (le virus occupant toute la capacité de travail du PC).
• Provoquer l'extinction de l'ordinateur à intervalles réguliers.
• ...

Comment les virus se transmettent-ils ?

Il existe plusieurs voies principales de contamination virale.

- Les clés USB qui passent d'ordinateur à ordinateur sont de très efficaces transporteurs de virus.
- Les CD-ROM sont moins sensibles car les virus ne peuvent pas s'y écrire.
- Les pièces jointes au courrier électronique sont également un vecteur bien connu. Il faut toutefois que la pièce jointe soit ouverte pour que le virus puisse s'activer.
- Le téléchargement de logiciels ou de fichiers de nature inconnue sur des sites non fiables peut amener des virus.
- Le téléchargement de logiciels piratés sur des réseaux comme eMule.
- ...

4. Quelle différence entre un ver et un virus ?

Un ver est un programme qui peut s'auto reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager; un ver est donc un virus réseau.
La plus célèbre anecdote à propos des vers date de 1988. Un étudiant (Robert T. Morris, de Cornell University) avait fabriqué un programme capable de se propager sur un réseau, il le lança et, 8 heures après l'avoir lâché, celui-ci avait déjà infecté plusieurs milliers d'ordinateurs. C'est ainsi que de nombreux ordinateurs sont tombés en panne en quelques heures car le "ver" (car c'est bien d'un ver dont il s'agissait) se reproduisait trop vite pour qu'il puisse être effacé sur le réseau. De plus, tous ces vers ont créé une saturation au niveau de la bande passante, ce qui a obligé la NSA à arrêter les connexions pendant une journée.

5. Les Chevaux de Troie :

Les Chevaux de Troie (Troyens ou " Trojan " en anglais) ont la particularité de se comporter comme les compagnons d'Ulysse : ils ouvrent des portes de l'ordinateur pour permettre à des personnes ou à d'autres logiciels malveillants d'entrer. Les Chevaux de Troie constituent une troisième sorte d'agent infectieux.

L'histoire du Cheval de Troie est bien connue. Après 10 années de siège de la ville de Troie, les Grecs construisent un cheval en bois dans lequel se cachent Ulysse et quelques compagnons.
Les Troyens, pensant que le Cheval est une offrande aux dieux, introduisent le Cheval à l'intérieur des fortifications de la ville. Durant la nuit, les guerriers sortent du cheval et ouvrent les portes de la ville, permettant ainsi sa prise par les Grecs.

En informatique, un " Cheval de Troie " (on dit aussi " Troyen " ou " Trojan " en anglais) est un logiciel malveillant qui se présente comme un programme utile ou une application intéressante.
La différence essentielle entre un " Troyen " et un ver réside dans le fait que le ver tente de se multiplier. Ce que ne fait pas le " Troyen ".

6. Autres nuisances logicielles

Les virus, vers et Chevaux de Troie constituent des nuisances importantes. D'autres types de logiciels, dont le but premier n'est pas de se propager d'un ordinateur à l'autre peuvent encore être ajoutés à la liste des problèmes possibles. Nous envisagerons ici d'évoquer les spywares, adwares, key loggers et dialers.

a- Les spywares (ou espiogiciels)

Comme leur nom l'indique, les spywares sont des logiciels dont l'objectif premier est d'espionner.
Le spyware est un logiciel ou un composant d'un logiciel qui collecte des informations sur l'utilisateur d'un ordinateur et les envoie vers son concepteur ou un commanditaire. Vous visitez tel site web, vous vous attardez sur telle page qui présente tel article en vente. Le spyware en prend bonne note et envoie ces informations vers un serveur. Un peu plus tard, vous travaillez calmement sur votre ordinateur, quand une publicité pour un produit similaire apparaît. Sans que vous ayez rien demandé. Vous fermez la fenêtre publicitaire. Deux minutes plus tard, elle revient.

Certains spywares sont intégrés, plus ou moins discrètement, à des logiciels gratuits. D'autres tentent de s'installer simplement lors de la visite d'une page web.

b- Les adwares (ou pubgiciel)

Les " adwares " sont des logiciels du même type que les spywares. Ils s'installent généralement sans que l'utilisateur ait bien pris conscience du fait qu'il installe un tel logiciel. Ces logiciels ajoutent des publicités dans les pages web visitées ou dans des fenêtres séparées. A la différence des spywares, les adwares ne communiquent pas d'information vers un serveur. Ils peuvent donc travailler même si l'ordinateur qu'ils colonisent n'est pas connecté à l'Internet.

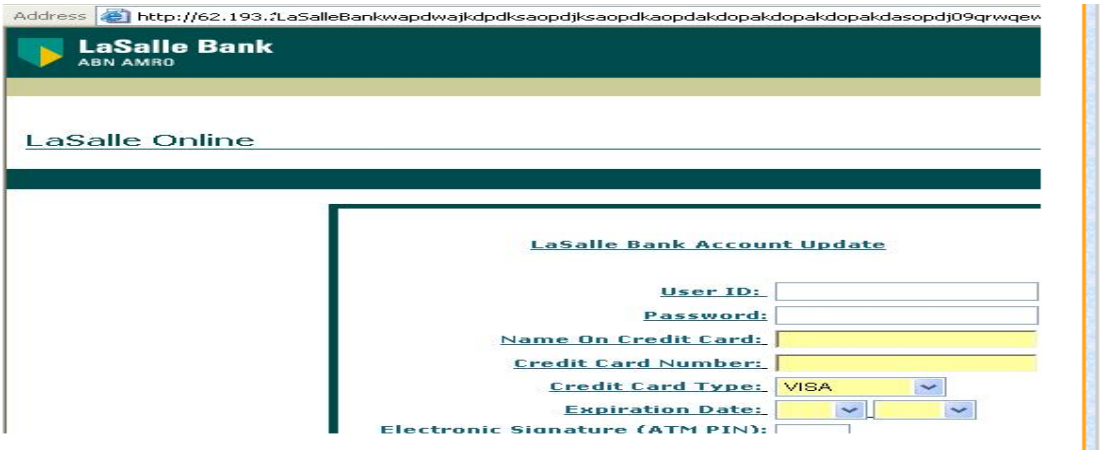
c- Le "phishing" (ou hameçonnage)

Le " phishing " est une technique par laquelle des malfaiteurs tentent d'entraîner un client d'une banque vers un site web qui ressemble très fort à celui de sa banque. Ils persuadent la personne de fournir son numéro de carte de crédit et le mot de passe qui y est associé. Ce qui leur permet ensuite très facilement de faire des achats ou de retirer de l'argent sur le compte en banque de leur victime.

Exemple de " phishing "

Le " phishing " ne cible généralement pas les clients connus d'une banque. Les malfaiteurs envoient des courriers électroniques, en utilisant les mêmes techniques que les spammeurs. Parmi les personnes qui reçoivent le courrier électronique, certaines sont réellement clientes d'une banque cible. Dans l'exemple ci-dessous, les victimes sont averties de la mise en service d'un nouveau système de sécurité et sont invitées à mettre leur compte à jour pour pouvoir en profiter.

Lorsque la victime clique sur le bouton " Continue ", au bas du message qu'elle a reçu, elle aboutit sur un site web qui ressemble à s'y méprendre au site web de la banque.



Elle est invitée à y fournir des informations relatives à sa carte de crédit. Le problème est qu'il ne s'agit pas du site web de la banque, mais d'une copie conforme. Si le client fournit les informations demandées, celles-ci sont alors transmises aux malfaiteurs.

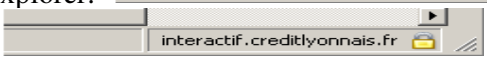
Dans le cas présenté ci-dessus, certains indices montrent clairement aux internautes avisés qu'il s'agit d'une supercherie :

• L'adresse URL de la banque ne figure pas dans la barre d'adresse ; à la place, on y trouve une adresse IP 

dont on vérifiera aisément qu'elle ne correspond pas à la banque.
• La connexion vers la banque n'est pas sécurisée : le protocole utilisé est simplement http et non https, comme il se devrait dans la communication de données confidentielles à une banque.

On ne trouve pas le  symbole de la connexion sécurisée dans le navigateur:

• Internet Explorer: 

• Firefox : 

• Dans certains cas, les pirates cachent l'adresse de destination à l'aide d'un petit programme qui superpose un rectangle où figure la vraie adresse de la banque.
La technique est d'ailleurs parfois imparfaite, comme sur l'exemple ci-dessous ou le " cache " apparaît bien (l'adresse URL est un peu décalée vers le bas) :

Il ne faut donc, en aucun cas, donner suite à des courriers électroniques censés provenir d'une banque ou de tout autre organisme qui vous demande de donner votre numéro de carte de crédit ou toute autre information confidentielle dans une simple connexion à l'Internet.

d- Le "spamming" (ou pourriel)

Spam : Le spam, autrement appelé spamming, pourriel (mot-valise de "poubelle" et "courriel"), ou polluriel (mot valise de "pollution" et "courriel" désigne un courriel anonyme, non sollicité et envoyé en masse à des fins publicitaires ou malhonnêtes.

L'objet du spam est très souvent publicitaire, mais il peut aussi s'agir de message politique, d'appel à la charité, d'arnaque financière, de chaînes ou d'hameçonnage (phishing en anglais). Dans ce dernier cas, le spam imite un message d'un service protégé par un mot de passe habituellement utilisé par le destinataire. Il a pour but de récupérer ses données personnelles (mot de passe, numéro de carte bancaire).
Les mailings ou newsletters publicitaires auxquels les internautes ont souscrit, même sans s'en rendre compte ne sont pas considérés comme des spams.

Le spam est souvent envoyé depuis des adresses volées qui masquent le véritable expéditeur. Le but est qu'il puisse être confondu avec les messages habituellement échangés par le destinataire.
L'envoi de spam est une activité frauduleuse sanctionnée par la loi française et interdite par plusieurs directives européennes

e- Les hoaxs (canulars)

De nombreux courriers électroniques circulent pour nous informer de faits graves, importants, urgents... mais souvent inexistants. Il s'agit souvent de courriers de type " chaînes " que vous êtes invité à relayer vers tout votre carnet d'adresses.

Il ne faut jamais renvoyer ces messages pour une simple raison mathématique. Imaginons que chaque personne qui reçoit un message de ce type le renvoie à 20 personnes qui se trouvent dans son carnet d'adresses.
Chaque personne en deuxième rang renvoie vers 20 destinataires. Nous aurons ainsi 400 messages envoyés. On peut aisément compter le nombre de messages qui transiteront sur l'Internet après quelques heures.

L'effet obtenu sera simplement une saturation du réseau.

f- Autres dangers et pestes de l'Internet

L'utilisation de l'Internet mène à rencontrer d'autres dangers et inconvénients. Certains ont déjà été cités. Tentatives d'intrusion dans votre ordinateur

Il existe plusieurs raisons pour lesquelles un " pirate " peut tenter d'entrer dans votre ordinateur et en prendre le contrôle :

- Utilisation de votre ordinateur pour envoyer des spams ;
- Utilisation de votre ordinateur pour lancer une attaque de grande envergure contre les serveurs d'une société précise.
- Utilisation de votre ordinateur pour entrer dans un autre ordinateur d'une Société ou d'un organisme d'Etat (CIA, FBI, banque, armée,...) sans laisser de traces autres que... les vôtres.

• Simple amusement à l'idée de vous voir impuissant devant votre ordinateur qui " travaille tout seul " : mouvements de la souris, ouverture et fermeture de fenêtres, messages à l'écran, ouverture du lecteur de CD,...

Une seule solution : fermer toutes les portes.

Certains comportements lors de l'utilisation de l'Internet ne sont pas sans poser de problèmes à cause des dangers qu'ils représentent.

• Visite de certains sites web pornographiques : dangers pour les adwares et les dialers.
• Téléchargements sur les réseaux d'échanges de fichiers : danger de télécharger n'importe quelle peste : virus, ver, adware,...
• Téléchargement de logiciels gratuits : ces logiciels sont souvent payés par les publicités qu'ils afficheront sur votre écran.
• Les logiciels libres, par contre, sont souvent gratuits mais ne posent pas ce type de problème.
• Utilisation de l'ordinateur sans antivirus (parfaitement à jour) et/ou sans pare-feu.
• Ouverture de n'importe quel courrier électronique dont vous ne connaissez pas l'auteur.
• Ouverture des pièces jointes aux courriers électroniques, même si l'on connaît l'auteur. Un virus ou un ver peut s'auto-envoyer en volant l'identité d'une personne que vous connaissez bien.
• …..